IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

IN RE LANSING COMMUNITY COLLEGE DATA BREACH LITIGATION	Master File No. 1:23-cv-00738-PLM Hon. Paul L. Maloney CONSOLIDATED ACTION

PLAINTIFFS' OPPOSITION TO
DEFENDANT LANSING COMMUNITY COLLEGE'S MOTION TO DISMISS

ISSUES PRESENTED

1. Should this Court deny Defendant's Motion to Dismiss Plaintiffs' Complaint pursuant to Fed. R. Civ. P. 12(b)(1) where Plaintiffs have Article III standing and allege a cognizable injury related to Defendant's Data Breach?

   Plaintiffs' Answer: Yes

2. Should this Court deny Defendant's Motion to Dismiss Plaintiffs' Complaint pursuant to Fed. R. Civ. P. 12(b)(6) where Plaintiffs sufficiently allege a breach of contract upon which relief may be granted?

   Plaintiffs' Answer: Yes

3. Should this Court deny Defendant's Motion to Dismiss Plaintiffs' Complaint pursuant to Fed. R. Civ. P. 12(b)(6) where Plaintiffs sufficiently allege unjust enrichment in the alternative to their contract claims upon which relief may be granted?

   Plaintiffs' Answer: Yes

4. Should this Court deny Defendant's Motion to Dismiss Plaintiffs' Complaint pursuant to Fed. R. Civ. P. 12(b)(6) where Plaintiffs sufficiently allege damages arising out of the Data Breach?

   Plaintiffs' Answer: Yes

MOST CONTROLLING AUTHORITY

- *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016)
- *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022)
- *Kostka v. Dickey's Barbecue Rests., Inc.*, 2022 WL 16821685 (N.D. Tex. Oct. 14, 2022)
- *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295 (2d Cir. 2021)
- *In re Marriott Intl., Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447 (D. Md. 2020)
- *Lochridge v. Quality Temp. Servs., Inc.*, No. 22-CV-12086, 2023 WL 4303577 (E.D. Mich. June 30, 2023)
- *Bates v. Green Farms Condo. Ass'n*, 958 F.3d 470 (6th Cir. 2020)

TABLE OF CONTENTS

I. INTRODUCTION 1

I. FACTUAL BACKGROUND 1

A. LCC's Collection of Plaintiffs' and Class Members' PII 1

B. The Data Breach Gives Rise to Plaintiffs' and Class Members' Damages 2

C. Plaintiffs' Damages Resulting from the Data Breach 3

III. LEGAL STANDARD 4

IV. ARGUMENT 5

A. The Court Should Disregard the Affidavit of Paul Schwartz 5

B. Plaintiffs Have Standing to Assert Their Claims 7

1. Plaintiffs Establish Standing Under Sixth Circuit Law and Follow the General Trend in Data Breach Jurisprudence 8
   a. Plaintiffs Satisfy the Injury Requirement of Article III Standing 8
   b. Plaintiffs' Injuries Are Traceable to Defendant's Conduct and Can Be Redressed by a Favorable Judicial Decision 13
   c. Plaintiffs and Class Members Can be Redressed by a Favorable Judicial Decision 15
   d. *Galaria* Remains Viable 15

2. Plaintiffs Satisfy the Standing Requirements Set Forth by *TransUnion* 21

C. Plaintiffs' Claims Survive Dismissal 23

1. Standard of Review Under Rule 12(b)(6) 23

2. Plaintiffs' Breach of Express Contract and Implied Contract Claims Survive Dismissal 23

3. Plaintiffs Adequately Plead Unjust Enrichment in the Alternative 26

V. CONCLUSION 29

TABLE OF AUTHORITIES

Cases

4041-49 W. Maple Condo. Ass'n v. Countrywide Home Loans, Inc.,
768 N.W.2d 88 (Mich. App. 2009) 24
Adkisson v. Jacobs Eng'g Grp., Inc.,
790 F.3d 641 (6th Cir. 2015) 5
Allen v. Wenco Mgmt., LLC,
No. 1:23 CV 103, 2023 WL 6456571 (N.D. Ohio Sept. 29, 2023) 19
Bates v. Green Farms Condo. Ass'n,
958 F.3d 470 (6th Cir. 2020) 6
Belle Isle Grill Corp. v. Detroit,
666 N.W.2d 271 (Mich. App. 2003) 28
Bowen v. Paxton Media Grp., LLC,
No. 5:21-CV-00143, 2022 WL 4110319 (W.D. Ky. Sept. 8, 2022) 20
Brickman v. Maximus, Inc.,
No. 2:21-CV-3822, 2022 WL 16836186 (S.D. Ohio May 2, 2022) 20
Buchholz v. Meyer Njus Tanick, PA,
946 F.3d 855 (6th Cir. 2020) 16
Burns v. United States,
542 F. App'x 461 (6th Cir. 2013) 7
Cascade Elec. Co. v. Rice,
245 N.W.2d 774 (Mich. App. 1976) 25
Chapman v. Nat'l Health Plans & Benefits Agency, LLC,
619 F. Supp. 3d 788 (E.D. Mich. 2022) 4
Clapper v. Amnesty Int'l USA,
568 U.S. 398 (2013) 9
Dennis v. MyLife.Com, Inc.,
No. 20-cv-954, 2021 WL 6049830 (D. N.J. Dec. 20, 2021) 22
Dickson v. Direct Energy, LP,
69 F.4th 338 (6th Cir. 2023) 8
Dinerstein v. Google, LLC,
484 F. Supp. 3d 561 (N.D. Ill. 2020), *aff'd as modified*, 73 F.4th 502 (7th Cir. 2023) 26
Directv, Inc. v. Treesh,
487 F.3d 471 (6th Cir. 2007) 23
Donovan v. FirstCredit, Inc.,
983 F.3d 246 (6th Cir. 2020) 8
Enslin v. The Coca-Cola Co.,
136 F. Supp. 3d 654 (E.D. Pa. 2015) 25
Envolve Pharmacy Sols., Inc. v. Rite Aid Headquarters Corp.,
No. N19C-12-214 PRW CCLD, 2023 WL 2547994 (Del. Super. Ct. Mar. 17, 2023) 26
Fraser v. Collier Const. Co.,
8 N.W.2d 889 (Mich. 1943) 25
Galaria v. Nationwide Mut. Ins. Co.,
663 F. App'x 384 (6th Cir. 2016) ..... *passim*

Garland v. Orlans, PC,
999 F.3d 432 (6th Cir. 2021) 16
Grainger, Jr. v. Cnty. of Ottawa,
No. 1:19-cv-501, 2021 WL 790771 (W.D. Mich. Mar. 2, 2021) 4, 5
Health Call of Detroit v. Atrium Home & Health Care Servs., Inc.,
706 N.W.2d 843 (Mich. App. 2005) 24
In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.,
No. CV 19-MD-2904, 2021 WL 5937742 (D. N.J. Dec. 16, 2021) 15
In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,
440 F. Supp. 3d 447 (D. Md. 2020) 12, 25
In re Moon's Est.,
188 N.W. 457 (Mich. 1922) 25
In re Rutter's Inc. Data Sec. Breach Litig.,
511 F. Supp. 3d 514 (M.D. Pa. 2021) 25
In re SuperValu, Inc.,
870 F.3d 763 (8th Cir. 2017) 15
In re USAA Data Sec. Litig.,
621 F. Supp. 3d 454 (S.D.N.Y. 2022) 22
Jones v. Ohio Bureau of Workers' Comp.,
2011-Ohio-1855 (Ct. Cl.) 19
Kanuszewski v. Michigan Dep't of Health & Hum. Servs.,
927 F.3d 396 (6th Cir. 2019) 17
Kingen v. Warner Norcross + Judd LLP,
No. 1:22-cv-01126-PLM-RSK (W.D. Mich.) 20, 25, 28
Kostka v. Dickey's Barbecue Rests., Inc.,
No. 3:20-CV-03424-K, 2022 WL 16821685 (N.D. Tex. Oct. 14, 2022), *report and recommendation adopted*, 2022 WL 16821665 (N.D. Tex. Nov. 8, 2022) 22
Kreipke v. Wayne State Univ.,
807 F.3d 768 (6th Cir. 2015) 23
Lee v. Belvoir Media Grp., LLC,
No. 22-12153, 2023 WL 6304682 (E.D. Mich. Sept. 27, 2023) 6
Lewert v. P.F. Chang's China Bistro, Inc.,
819 F.3d 963 (7th Cir. 2016) 9
Lexmark Intern., Inc. v. Static Control Components, Inc.,
572 U.S. 118 (2014) 13
Lochridge v. Quality Temp. Servs., Inc.,
No. 22-cv-12086, 2023 WL 4303577 (E.D. Mich. June 30, 2023) 12, 20
Longenecker-Wells v. Benecard Servs. Inc,
658 F. App'x 659 (3d Cir. 2016) 25
Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992) 8
Lyshe v. Levy,
854 F.3d 855 (6th Cir. 2017) 17
Mackey v. Belden, Inc.,
No. 4:21-cv-00149, 2021 WL 3363174 (E.D. Mo. Aug. 3, 2021) 25

Max Arnold & Sons, LLC v. W.L. Hailey & Co., Inc.,
452 F.3d 494 (6th Cir. 2006) 6
McKenzie v. Allconnect, Inc.,
369 F. Supp. 3d 810 (E.D. Ky. 2019) 10
McMorris v. Carlos Lopez & Assocs., LLC,
995 F.3d 295 (2d Cir. 2021) 8, 9, 22
Mills v. Barnard,
869 F.3d 473 (6th Cir. 2017) 23
Mitchell v. BMI Fed. Credit Union,
374 F. Supp. 3d 664 (S.D. Ohio 2019) 4
Newman v. Total Quality Logistics, LLC,
2021 WL 1192669 (S.D. Ohio Mar. 30, 2021) 19
Norton v. Beasley,
No. 21-6053, 2022 WL 17348385 (6th Cir. 2022) 16
Parsons v. U.S. Dept. of Justice,
801 F.3d 701 (6th Cir. 2015) 13
Passa v. City of Columbus,
123 F. App'x 694 (6th Cir. 2005) 6
Polselli v. U.S. Dep't of the Treasury–Internal Revenue Serv.,
23 F.4th 616 (6th Cir. 2022) 5
Rogers v. Stratton Indus., Inc.,
798 F.2d 913 (6th Cir. 1986) 5
Sackin v. TransPerfect Glob., Inc.,
278 F. Supp. 3d 739 (S.D.N.Y. 2017) 25, 27
Safety Specialty Ins. Co. v. Genesee Cnty. Bd. of Comm'rs,
53 F.4th 1014 (6th Cir. 2022) 16
Salas v. Acuity-CHS, LLC,
No. CV 22-317-RGA, 2023 WL 2710180 (D. Del. Mar. 30, 2023) 22
Saleh v. Barr,
801 Fed. Appx. 384 (6th Cir. 2020) 18, 19
Savidge v. Pharm-Save, Inc.,
570 F. Supp. 3d 518 (W.D. Ky. 2021) 10
Smallman v. MGM Resorts Int'l,
638 F. Supp. 3d 1175 (D. Nev. 2022) 12
Spokeo, Inc. v. Robins,
578 U.S. 330 (2016) 8
Thomas v. TOMS King (Ohio), LLC,
997 F.3d 629 (6th Cir. 2021) 16
TransUnion LLC v. Ramirez,
141 S. Ct. 2190 (2021) 20, 21, 22
Tucker v. Marietta Area Health Care, Inc.,
No. 2:22-cv-184, 2023 WL 423504 (S.D. Ohio Jan. 26, 2023) 26
Wittman v. Personhuballah,
578 U.S. 539 (2016) 15

Statutes

U.S. Const. art. III § 2 8

Other Authorities

7 Mich. Civ. Jur. Damages § 9 24

Rules

Fed. R. Civ. P. 12(b)(1) 4
Fed. R. Civ. P. 12(b)(6) 4
Fed. R. Civ. P. 12(d) 6
Fed. R. Civ. P. 56(c) 5

Treatises

Wright & Miller, Fed. Prac. & Proc. Civ. § 1350 (3d ed. 2023) 5

I. INTRODUCTION

This lawsuit stems from a massive and preventable data breach spanning from December 25, 2022, through March 15, 2023, during which cybercriminals infiltrated Lansing Community College's ("Defendant" or "LCC") inadequately-protected data systems and gained access to the highly sensitive personally identifiable information ("PII") of approximately 757,832 individuals ("the Class" or "Class Members") (the "Data Breach" or "Breach"). As a result of LCC's failure to implement adequate data security, Plaintiffs'[1] and Class Members' PII is now in the hands of cybercriminals who already have and will continue to misuse their PII for years to come. For the reasons stated herein, Defendant's Motion to Dismiss Plaintiffs' Consolidated Amended Class Action Complaint should be denied.

II. FACTUAL BACKGROUND

A. LCC's Collection of Plaintiffs' and Class Members' PII

LCC is "one of the largest community colleges in Michigan, serving more than 14,500 students per year." Consolidated Amended Class Action Compl. ("CAC") ¶ 2, ECF No. 18. Plaintiffs and Class Members are or were employees, students, applicants for admission, or applicants for employment of LCC. *Id.* ¶¶ 3, 26. Plaintiffs and Class Members were required to provide extensive amounts of their PII to LCC in order to obtain employment or admission to LCC. *Id.* ¶ 3. Plaintiffs provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep their PII confidential and secure from unauthorized access when they provided their PII to LCC. *Id.* ¶¶ 3, 27, 33. Unfortunately, Defendant failed to meet Plaintiffs' and Class Members' reasonable expectation

[1] "Plaintiffs" collectively refers to Plaintiffs Ivory Whitby, Sameer Shah, Gabriel Banish, William Barber, Lindsay Luoma, and Chelsea Lee Ouimette.

that Defendant would protect their PII, as such, Plaintiffs' and Class Members' PII is now in the hands of criminals.

B. The Data Breach Gives Rise to Plaintiffs' and Class Members' Damages

According to LCC, on or around March 14, 2023, LCC became aware of suspicious activity on its computer network. *Id.* ¶¶ 4, 34. In response, LCC shut down the college on March 15, 2023, for what LCC described as an "ongoing cybersecurity incident." *Id.* ¶¶ 5, 35. LCC advised students and most of its employees not to log onto the college's systems and or return to campus. *Id.* ¶ 5. The school shutdown and substantially disrupted the academic year and the lives of Plaintiffs and Class Members. *See id.* Indeed, most classes and activities were cancelled for the rest of the week due to the Breach. *Id.* At the time, LCC assured Plaintiffs and Class Members that "it had no evidence that employee or student information ha[d] been compromised." *Id.* ¶ 6. This assurance turned out to be false.

After an investigation, LCC determined that an unauthorized actor gained access to its data systems and had nearly three months of unfettered access to Plaintiffs' and Class Members' PII. *See id.* ¶¶ 7. The Data Breach spanned from December 25, 2022, through March 15, 2023, because LCC failed to detect the Breach until March 14, 2023. *See id.* ¶¶ 4, 7. To make matters worse, contrary to its initial assurances, LCC later revealed that Plaintiffs' and Class Members' PII was indeed compromised in the Data Breach. *Id.* ¶ 8. The types of PII compromised in the Data Breach included sensitive information such as full names and Social Security numbers—or in other words, everything a criminal needs to commit identity theft and fraud. *Id.* ¶ 1.

Acknowledging the present and continuing risk of harm Plaintiffs and Class Members faced after the Data Breach, Defendant mailed its "Notice of Security Incident" letters to the victims of the Data Breach on or around June 30, 2023, and offered to provide Plaintiffs and Class

Members with complimentary credit monitoring services. However, this warning letter arrived *much* too late—as described below, Plaintiffs and Class Members had already begun to experience the serious ramifications of the Data Breach as criminals had begun misusing the PII stolen in the Data Breach to their detriment.

C. Plaintiffs' Damages Resulting from the Data Breach

Following the Data Breach, Plaintiffs and Class Members experienced harm that is directly linked to LCC's Data Breach. For example, following the Data Breach, Plaintiff Ouimette experienced several instances of actual misuse of her PII, upending her life for months on end, including: (i) several unauthorized hard inquiries on her credit report; (ii) several fraudulent charges to her debit card (requiring her to obtain a replacement card); (iii) unauthorized charges on her credit card; (iv) identity theft in that an identity thief attempted to obtain a car loan in her name; and (v) numerous unsolicited spam calls and emails. *Id.* ¶¶ 165–66. As a result of the Data Breach and the harm caused therefrom, Plaintiff Ouimette was forced to file a police report, file a report with the Federal Trade Commission, and place a fraud alert on her credit. *Id.* ¶ 167. Plaintiff Ouimette estimates that she has spent approximately 84 hours responding to the ramifications of the Data Breach so far.

Further, Plaintiff Luoma also experienced actual fraud following the Data Breach. *Id.* ¶ 158. On or around March 22, 2022, an unauthorized individual filed a tax return in Plaintiff Luoma's name with the Internal Revenue Service ("IRS"). *Id.* ¶ 158. Plaintiff Luoma had to contact the IRS to report and dispute the fraudulent return and spent several hours placing holds on her credit and communicating with the IRS. *Id.* Additionally, following the Data Breach, Plaintiffs Barber and Banish obtained credit monitoring services to monitor their accounts and credit due to the harm LCC caused. *Id.* ¶¶ 144, 150. These harms are in addition to the other harms all Plaintiffs

allege, including: (i) invasion of privacy; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (iii) the loss of benefit of the bargain (price premium damages); (iv) diminution of value of their PII; (v) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII; and (vi) emotional distress. *Id.* ¶¶ 93, 127–29, 136–38, 143–45, 150–53, 158–60, 168–73.

The reality is that the harms described above are only the tip of the iceberg. Plaintiffs and Class Members are at an imminent risk of fraud and identity theft for the rest of their lives. As such, Defendant's Motion to Dismiss must be denied, and Defendant should be held to account for the everlasting consequences of its actions and inactions.

III. LEGAL STANDARD

Defendant moves to dismiss Plaintiffs' claims under Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction, and under Rule 12(b)(6), for failure to state a claim.

A motion to dismiss under Fed. R. Civ. P. 12(b)(1) tests if the Court has subject matter jurisdiction and, if a court lacks jurisdiction, it must dismiss the claims. Fed. R. Civ. P. 12(b)(1). A Rule 12(b)(1) motion "may challenge a federal court's subject matter jurisdiction through either a facial or factual attack." *Chapman v. Nat'l Health Plans & Benefits Agency, LLC*, 619 F. Supp. 3d 788, 791 (E.D. Mich. 2022). "A facial attack 'questions merely the sufficiency of the pleading[,]' and requires the district court to 'take[] the allegations in the complaint as true.'" *Mitchell v. BMI Fed. Credit Union*, 374 F. Supp. 3d 664, 667 (S.D. Ohio 2019) (citation omitted); *see also Grainger, Jr. v. Cnty. of Ottawa*, No. 1:19-cv-501, 2021 WL 790771, at *4 (W.D. Mich. Mar. 2, 2021) ("In a facial attack, the court accepts as true all the allegations in the complaint,

similar to the standard for a Rule 12(b)(6) motion."). "In a factual attack, a movant presents evidence outside of the pleadings to contest jurisdictional facts alleged in the petitions." *Polselli v. U.S. Dep't of the Treasury–Internal Revenue Serv.*, 23 F.4th 616, 621 (6th Cir. 2022); *see also* Wright & Miller, Fed. Prac. & Proc. Civ. § 1350 (3d ed. 2023) ("A factual challenge attacks the factual allegations underlying the assertion of jurisdiction, either through the filing of an answer or otherwise presenting competing facts."). "When challenged by a motion filed under Rule 12(b)(1), the plaintiff bears the burden of establishing subject matter jurisdiction." *Grainger, Jr.*, 2021 WL 790771, at *4.

A motion to dismiss under Rule 12(b)(6) tests the sufficiency of the Complaint and requires dismissal where the Complaint "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "When considering a Rule 12(b)(6) motion to dismiss for failure to state a claim, the district court must "construe the complaint in the light most favorable to the plaintiff and accept all factual allegations as true." *Adkisson v. Jacobs Eng'g Grp., Inc.*, 790 F.3d 641, 647 (6th Cir. 2015).

IV. ARGUMENT

A. THE COURT SHOULD DISREGARD THE AFFIDAVIT OF PAUL SCHWARTZ

As a threshold issue, the Court should disregard Paul Schwartz's affidavit (ECF No. 20-1, Ex. 1 to Def.'s Br.) because Defendant seeks to use it as a vehicle to improperly present facts. In its attempt to contest Plaintiffs' allegations, Defendant ignores that "in a Rule 12(b)(6) motion in which matters outside the record are relied upon . . . the moving party (here, [D]efendant[]) has the burden of showing there are no genuine issues as to any material facts, as the motion shall be treated as one for summary judgment." *Rogers v. Stratton Indus., Inc.*, 798 F.2d 913, 915 (6th Cir. 1986) (citing Fed. R. Civ. P. 56(c)). Without making any attempt to satisfy that burden, Defendant

attempts to introduce facts that run directly counter to those alleged in Plaintiffs. *See* ECF No. 20-1, PageID.331, ¶¶ 19-22 (Ex. 1 to Def.'s Br.). The Court should disregard the affidavit in its entirety because "it is black-letter law that, with a few irrelevant exceptions, a court evaluating a motion for judgment on the pleadings (or a motion to dismiss) must focus only on the allegations in the pleadings." *Bates v. Green Farms Condo. Ass'n*, 958 F.3d 470, 483 (6th Cir. 2020).

In the event that the Court does consider the affidavit, it must convert the motion to one for summary judgment and afford Plaintiffs "'a reasonable opportunity to present all the [pertinent] material.'" *Bates*, 958 F.3d at 484 (quoting Fed. R. Civ. P. 12(d)). As the Sixth Circuit has long held, "even a district court's failure to *expressly* reject evidence attached to the briefs triggers its duty to treat the motion as one for summary judgment." *Id*. (emphasis in original) (citing to *Max Arnold & Sons, LLC v. W.L. Hailey & Co., Inc.*, 452 F.3d 494, 502–04 (6th Cir. 2006).

Judge Kumar of the Eastern District of Michigan recently rejected a similar attempt by a defendant to introduce facts in support of its motion to dismiss for lack of standing and declined to consider the affidavit or to convert the motion in to one for summary judgement. *See Lee v. Belvoir Media Grp., LLC*, No. 22-12153, 2023 WL 6304682, at *2 (E.D. Mich. Sept. 27, 2023) (excluding the affidavit proffered to refute the plaintiffs' allegations). This Court should likewise refuse to consider the affidavit. But in the event the Court wishes to consider Mr. Schwartz's affidavit, Plaintiffs must be allowed to conduct discovery and challenge the contentions asserted therein. *Passa v. City of Columbus*, 123 F. App'x 694, 698 (6th Cir. 2005) ("As a result, the district court's determination that [the plaintiff] had not stated a claim was based on evidence, favorable to the [defendant], that it should not have considered without allowing [the plaintiff] the opportunity to respond.").

Finally, even if the Court were to consider the affidavit, it contains nothing more than Mr. Schwartz's say-so. Mr. Schwartz simply lists conclusions of fact without showing how those conclusions were reached, what methodologies were employed, and whether any such investigation was sufficient. *See* ECF No. 20-1, PageID.331, ¶¶ 19-22 (Ex. 1 to Def.'s Br.). Moreover, Mr. Schwartz's conclusions run directly counter to Plaintiffs' allegations. Compare, *e.g.*, *id*. with CAC ¶¶ 5, 10, 35, 37, 42, 158, 166. Because Mr. Schwartz's affidavit improperly attempts to contest the facts alleged in Plaintiffs' Complaint, it should be rejected entirely from consideration. *See Burns v. United States*, 542 F. App'x 461, 466 (6th Cir. 2013) (a dispute over the veracity of facts "disqualifies the exhibit from consideration on a motion to dismiss").

B. PLAINTIFFS HAVE STANDING TO ASSERT THEIR CLAIMS

Even if the Court decides to consider the facts alleged in Defendant's Affidavit, the Court should still find that Plaintiffs have standing and, therefore, survive Defendant's Rule 12(b)(1) motion to dismiss because, as explained in greater detail below, Plaintiffs satisfy the elements of standing. LCC appears to posture its Motion as a factual attack. *See* Def.'s Br., ECF No. 20, PageID.305-306 (suggesting that "there is a factual attack on the Court's jurisdiction"). However, the only purported "evidence" or "competing facts" Defendant has come forward with in support of its Motion is its Affidavit and Declaration of Paul Schwartz, which itself admits that "LCC's computer networks were attacked." *See* ECF No. 20-1, PageID.330 (Ex. 1 to Def.'s Br.). Defendant attempts to dispute the facts presented in Plaintiffs complaint by way of an Affidavit which provides contradictory facts that are unsupported. Moreover, the facts pleaded in Plaintiffs' Complaint satisfy the elements of standing. Accordingly, Defendants 12(b)(1) motion should be denied.

1. Plaintiffs Establish Standing Under Sixth Circuit Law and Follow the General Trend in Data Breach Jurisprudence

Article III of the Constitution limits federal courts' jurisdiction to actual cases or controversies, *see* U.S. Const. art. III § 2, and "[a]n essential component of the case-or-controversy requirement is the doctrine of standing, which 'limits the category of litigants empowered to maintain a lawsuit in federal court to those who seek redress for a legal wrong.'" *Dickson v. Direct Energy, LP*, 69 F.4th 338, 342 (6th Cir. 2023) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016)). To establish standing, a plaintiff must show "(1) a concrete and particularized injury-in-fact which (2) is traceable to the defendant's conduct and (3) can be redressed by a favorable judicial decision." *Id.* at 343 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)). Here, Plaintiffs have suffered an "injury in fact," their injuries are traceable to the Data Breach, and their injuries are redressable by a favorable judicial decision. *See Spokeo*, 578 U.S. at 338; *Donovan v. FirstCredit, Inc.*, 983 F.3d 246, 251 (6th Cir. 2020); *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 299-300 (2d Cir. 2021); *see also Lujan*, 504 U.S. at 561 ("At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice.").

a. Plaintiffs Satisfy the Injury Requirement of Article III Standing

The first element of standing—injury in fact—does not impose a particularly heavy burden on plaintiffs. In the data breach context, the Sixth Circuit has found that allegations of personal data theft in a cyber-attack, coupled with reasonably incurred time and expense spent on mitigating the damages associated with theft of an individual's PII, are sufficient to establish a concrete injury. *See Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) ("Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are

sufficient to establish a cognizable Article III injury at the pleading stage of the litigation").[2] In *Galaria*, the plaintiffs alleged "that the theft of their personal data places them at a continuing, increased risk of fraud and identity theft beyond the speculative allegations of 'possible future injury' or 'objectively reasonable likelihood' of injury that the Supreme Court has explained are insufficient." *Id.* at 388 (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410-14 (2013)).

The Sixth Circuit recognized that "[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals," and "although it might not be 'literally certain' that [the p]laintiffs' data will be misused . . . it would be unreasonable to expect Plaintiffs to wait for actual misuse . . . before taking steps to ensure their own personal and financial security." *Id.*; *see also Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016) ("It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is sooner or later to make fraudulent charges or assume those consumers' identities.") (quotation marks omitted); *McMorris*, 995 F.3d at 301; *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 156-57 (3d Cir. 2022) (confirming that class members whose sensitive data was disseminated to unauthorized third parties suffer a concrete harm that qualifies as an injury in fact, and concluding that this alleged injury in fact was "far more imminent" where a hacker group accessed the plaintiff's sensitive information and published the information on the dark web). This is especially true where the target of the attack affirmatively recommends taking these steps as here, *see Galaria*, 663 F. App'x at 388, and when the data is of the type "that could be used to perpetrate identity theft or fraud" such as financial information,

[2] In *Galaria*, the plaintiffs brought class actions against Nationwide after hackers breached its computer network and stole their personal information. *See Galaria*, 663 F. App'x at 385. The district court dismissed the complaints, concluding, in part, that the plaintiffs lacked Article III standing. *See id.* However, in a consolidated appeal, the Sixth Circuit reversed the district court's ruling, holding that the plaintiffs did in fact have Article III standing. *Id.*

Social Security Numbers, dates of birth, addresses, and other categories of PII—the exact type of sensitive data breached here. *Clemens*, 48 F.4th at 156-57.

The complaints in *Galaria* alleged that the plaintiffs "must expend time and money to monitor their credit, check their bank statements, and modify their financial accounts." *Id.* The Sixth Circuit ultimately found that "these costs are a concrete injury suffered to mitigate an imminent harm, and satisfy the injury requirement of Article III standing." *Id.* at 389; *see also Savidge v. Pharm-Save, Inc.*, 570 F. Supp. 3d 518, 522 (W.D. Ky. 2021) ("Plaintiffs' reasonably incurred out-of-pocket expenses constitute a cognizable injury."); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019) (following *Galaria* and finding that the plaintiffs' lost time and money expended to protect their personal data from misuse constitute a cognizable injury for Article III standing purposes).

Just like the plaintiffs in *Galaria*, Plaintiffs here sufficiently allege that the theft of their PII places them at a continuing, increased risk of fraud and identity theft. Specifically, Plaintiffs allege that "[a]s a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent." CAC ¶ 93; *see also id.* at ¶¶ 94-98 (the Data Breach increases Plaintiffs' and Class Members' risk of identity theft).

Plaintiffs also—just like the plaintiffs in *Galaria*—sufficiently allege that they must expend time and expenses to mitigate the risks of identity theft and fraud. All Plaintiffs took steps to monitor their accounts for fraudulent activity and anticipate spending additional time-consuming steps in the future to help mitigate the harm caused by the Data Breach, including continually reviewing their accounts for fraudulent activity. *See id.* at ¶¶ 93, 99-104 (loss of time

to mitigate the risk of identity theft and fraud), ¶ 113 (constant surveillance and monitoring of personal and financial records), ¶¶ 116-120 (cost of credit and identity theft monitoring is reasonable and necessary); *see also id.* at ¶¶ 127-30 (Plaintiff Whitby spent significant time dealing with the potential effects and incidents resulting from the Data Breach), ¶¶ 136-37 (Plaintiff Shah has expended a significant amount of time taking steps to mitigate the adverse consequences of the Data Breach); ¶¶ 143-44 (Plaintiff Banish spent hours monitoring his accounts and signed up for credit monitoring through Experian); ¶¶ 150-53 (Plaintiff Barber purchased credit and fraud monitoring through Discover, including Fraud & Security Protections, identity monitoring, and online privacy protection at a cost of $15.00 per month, and spent hours taking steps to mitigate the effects of the Data Breach); ¶¶ 158-59 (Plaintiff Luoma experienced tax fraud, when an unauthorized individual filed a tax return in Plaintiff Luoma's name with the IRS, which required her to place holds on her accounts and spend significant time addressing this instance of fraud, as well as pay $30 in postage to mail her tax return to the IRS); ¶¶ 165-169 (Plaintiff Ouimette had several unauthorized hard inquiries on her credit reports, several unauthorized fraudulent charges on her debit card requiring her to obtain a replacement, unauthorized fraudulent charges on her credit cards, identity theft in the form of an unauthorized car loan in her name, an increased number of unsolicited spam emails and texts, was forced to place fraud alerts on her credit, and has expended over 80 hours mitigating the effects of the Data Breach). LCC's argument that "alleged future harm does not rise to the level of injury in fact" (Def.'s Br., ECF No. 20, PageID.318) is belied by the CAC allegations that Plaintiffs have *already* taken steps to ameliorate or otherwise mitigate the harms caused by the Data Breach, including by spending significant time and effort monitoring their accounts for suspicious activity and expending money out-of-pocket to purchase identity theft protection services. CAC, ¶¶ 122-173.

Further, also like the defendant in *Galaria*, who recommended that the plaintiffs take steps to ensure their own personal and financial security, *see Galaria*, 663 F. App'x at 388, LCC itself has recognized that injury is certainly impending because it is offering 12 months of identity monitoring services and is encouraging Plaintiffs and Class Members to monitor their financial accounts for many years to mitigate the risk of identity theft. *See id.* at ¶¶ 65-66, 100; *see Lochridge v. Quality Temp. Servs., Inc.*, No. 22-CV-12086, 2023 WL 4303577, at *4 (E.D. Mich. June 30, 2023) ("It would be unreasonable to expect Plaintiffs to wait for actual misuse before taking these mitigation steps, especially when they were specifically suggested by Defendant in the notification letter.").

Additionally, "Plaintiffs sufficiently allege details about the existence of an economic market for selling stolen PII, including the fact that PII can be bought and sold at identifiable prices on established markets." *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022); *see also* CAC ¶ 76, 96, 105-115. Plaintiffs' allegations that the Data Breach resulted in a diminution in value of their PII are well-pleaded, *see id.* at ¶¶ 93, 105-115, as "the Data Breach devalued Plaintiffs' PII by interfering with their fiscal autonomy" and "[a]ny past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace." *Smallman*, 638 F. Supp. 3d at 1191; *see also In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("[T]he value of consumer personal information is not derived solely . . . by its worth in some imagined market place where the consumer actually seeks to sell it to the highest bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check.").

These allegations go "beyond . . . speculative allegations of 'possible future injury' or 'objectively reasonable likelihood' of injury," and "[t]his is not a case where Plaintiffs seek to 'manufacture standing by incurring costs in anticipation of non-imminent harm.'" *Galaria*, 663 F. App'x at 388-89. LCC's claims that "Plaintiffs make no plausible allegations of impending data misuse" (Def.'s Br., ECF No. 20, PageID.320) blatantly ignores the allegations in Plaintiffs' CAC. LCC minimizes the existence of the present injuries and cognizable economic harm suffered by Plaintiffs. Plaintiffs' damages are real and compensable. Accordingly, Plaintiffs have established a cognizable Article III injury.

b. Plaintiffs' Injuries Are Traceable to Defendant's Conduct and Can Be Redressed by a Favorable Judicial Decision

The Sixth Circuit has held that the second element of standing—traceability—"requires 'more than speculative but less than but-for' causation." *Galaria*, 663 F. App'x at 390. This element "is not focused on whether the defendant caused the plaintiff's injury in the liability sense;" rather, this requirement "mainly serves to eliminate those cases in which a third party and not a party before the court causes the injury." *Id.* (citations and quotation marks omitted); *see also Parsons v. U.S. Dept. of Justice*, 801 F.3d 701, 715 (6th Cir. 2015) ("[C]ausation to support standing is not synonymous with causation sufficient to support a claim."); *Lexmark Intern., Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of Article III standing."). In *Galaria*, the plaintiffs alleged that Nationwide "failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and other Class Members' data to protect against anticipated threats to the security or integrity of such information." *Galaria*, 663 F. App'x at 390 (quotation marks omitted). The Sixth Circuit found that these allegations met the traceability threshold for Article III standing. In reaching its decision, the court recognized that "[a]lthough

hackers are the direct cause of Plaintiffs' injuries, the hackers were able to access Plaintiffs' data only because [the defendant] allegedly failed to secure the sensitive personal information entrusted to its custody. In other words, but for [the defendant]'s allegedly lax security, the hackers would not have been able to steal Plaintiffs' data." *Id.*

Here, Plaintiffs likewise allege that LLC "failed to adequately protect Plaintiffs' and Class Members' PII," that LCC "failed to even encrypt or redact this highly sensitive information," and that "[t]his unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect Class Members' sensitive data." CAC ¶ 10; *see also* ¶ 41 ("Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members causing the exposure of their PII."); ¶ 44 (Defendant did not use reasonable security procedures and practices); ¶ 54 ("Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members."); ¶ 79-87 (Defendant failed to comply with FTC guidelines); ¶ 88-92 (Defendant failed to comply with industry standards). Plaintiffs further allege that LCC's failure to implement such procedures and protocols resulted in an unauthorized actor obtaining access to highly sensitive PII data of approximately 757,835 individuals, that the unauthorized actor had access to that data for approximately two and a half months before LCC discovered the breach, and that after the breach was discovered, LCC delayed over three months in alerting Plaintiffs to the breach. *Id.* at ¶¶ 1-10, 38.

LCC's various fact-laden arguments, including arguing that none of the "fraudulent activity was *caused* by the Cybersecurity Incident" (Def.'s Br., ECF No. 20, PageID.318 (emphasis Defendant's)) fail to acknowledge the facts pled above—and "[w]hile a mere 'speculative chain

of possibilities' cannot establish traceability . . . even 'an indirect causal relationship' can be sufficient to meet this standard." *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, No. CV 19-MD-2904, 2021 WL 5937742, at *11 (D. N.J. Dec. 16, 2021) (quotation omitted). Plaintiffs allege that LCC "knew or should have known that [its] data security was insufficient . . . and should have maintained better oversight over [its] data security practices" and that Plaintiffs were injured as a result of these alleged acts and omissions. *Id.* at *12. These allegations are "enough to allege that their injuries were caused by—and fairly traceable to—Defendant['s] conduct." *Id.*; *see also In re SuperValu, Inc.*, 870 F.3d 763, 772 (8th Cir. 2017) (At the motion to dismiss stage "we presume that these general allegations embrace those specific facts that are necessary to support a link between [the] fraudulent charge and the data breaches.").

c. Plaintiffs and Class Members Can be Redressed by a Favorable Judicial Decision

With respect to the third element—redressability—Plaintiffs' injuries "will likely be redressed by a favorable decision." *Galaria*, 663 F. App'x at 391 (quoting *Wittman v. Personhuballah*, 578 U.S. 539, 543 (2016)). Like the *Galaria* plaintiffs, Plaintiffs here are seeking "compensatory damages for their injuries, and a favorable verdict would provide redress." *See id.*; CAC ¶¶ 194, 208, 225; *see also* CAC at Prayer for Relief, PageID.275-279.[3]

d. *Galaria* Remains Viable

Defendant contends that the Sixth Circuit has "continued to grapple" with "future risk of harm" opinions after *Galaria* and cherry-picks cases to support an argument that Plaintiffs "have only pled speculative future harm that is not an injury-in-fact." *See* Def.'s Br., ECF No. 20, PageID.312-313. However, Defendant fails to cite a single *data breach* case from the Sixth Circuit

[3] In addition to their claims for damages, Plaintiffs seek injunctive relief. *See* ¶¶ 195, 209.

to support this argument[4] and none of the cases Defendant cites even mention, let alone discuss *Galaria*. *See id.*; *see also Buchholz v. Meyer Njus Tanick, PA*, 946 F.3d 855 (6th Cir. 2020) (action against debt collector under Fair Debt Collection Practices Act); *Norton v. Beasley*, No. 21-6053, 2022 WL 17348385, at *1 (6th Cir. 2022) (action by property owners to have their real properties unlisted from National Register of Historic Places); *Safety Specialty Ins. Co. v. Genesee Cnty. Bd. of Comm'rs*, 53 F.4th 1014, 1018 (6th Cir. 2022) (claims to recover surplus proceeds seized from tax foreclosure and for declaration of no duty to defend or indemnify); *Garland v. Orlans, PC*, 999 F.3d 432 (6th Cir. 2021) (action for violation of Fair Debt Collection Practices Act and Michigan's Regulation of Collections Practices Act).

Rather, a better understanding of how the Sixth Circuit has grappled with "future risk of harm" opinions following *Galaria* entails a review of Sixth Circuit opinions that specifically discuss *Galaria.* For instance, in *Thomas v. TOMS King (Ohio), LLC*, 997 F.3d 629 (6th Cir. 2021), a consumer brought a class action against a restaurant under the Fair and Accurate Credit Transaction Act ("FACTA") after receiving a printed receipt with the first six and last four digits of her credit card number. *See id.* at 632. The "truncation requirement" of FACTA prohibits anyone who accepts credit or debit card payments from printing more than the last five digits of a consumer's card number on the receipt, and the question before the court was whether the defendants' violation of FACTA resulted in harm sufficiently concrete for Article III standing purposes. *See id.* The Sixth Circuit ultimately held that "a violation of the truncation requirement does not automatically cause an injury in fact," and that the plaintiff's complaint failed "to establish that Defendants' technical violation of the statute caused harm or presented any material risk of

[4] Defendant concedes this fact in its Motion. *See* Def.'s Br., ECF No. 20, PageID.312 ("After *Galaria*, the Sixth Circuit has continued to grapple with when a 'future risk of harm' creates standing *outside of the data breach realm*.") (emphasis added).

harm." The court found that the allegations in the plaintiff's complaint did "not establish an increased risk of identity theft . . . because they do not show how, even if [the p]laintiff's receipt fell into the wrong hands, criminals would have a gateway to consumers' personal and financial data." *Id.* at 640. In reaching its decision, the Sixth Circuit compared the facts before it to its prior decision in *Galaria*, and reiterated its holding that "the alleged theft of the [*Galaria*] plaintiffs' personal information constituted 'a substantial risk of harm, coupled with reasonably incurred mitigation costs,' because the alleged violation of the statute created a concrete risk that their data would be used for fraudulent purposes." *Id.* at 642. The Sixth Circuit stated that "[t]he comparison highlights what's missing in [*Thomas*]: an allegation that the information revealed . . . created a substantial risk that criminals could parlay that information into actual identity theft."

Distinct from *Thomas*—and consistent with *Galaria*—the Plaintiffs' Complaint here is replete with allegations that the Data Breach has created a substantial risk that criminals could parlay Plaintiffs' PII into actual identity theft. *See, e.g.*, CAC at ¶¶ 94-98 (alleging that the Data Breach increases Plaintiffs' and Class Members' risk of identity theft); *see also Kanuszewski v. Michigan Dep't of Health & Hum. Servs.*, 927 F.3d 396, 410-11 (6th Cir. 2019) (citing *Galaria*, 663 F. App'x at 388) ("[I]t is not too speculative to assert that the state or third parties may conduct chemical analysis on the blood samples—indeed, Plaintiffs allege that this is the very reason why the state retains the samples and why third parties wish to obtain them.").

Similarly, in *Lyshe v. Levy*, 854 F.3d 855 (6th Cir. 2017), a debtor brought a suit under the Fair Debt Collection Practices Act ("FDCPA") against a debt collection agency, alleging that the agency violated the FDCPA by failing to provide electronic discovery without prompting and requiring that the responses to the requests for admission be sworn and notarized. *See id.* at 856-57. On appeal, the only disputed issue was whether the debtor suffered an injury in fact. *See id.* at

857. The Sixth Circuit concluded that "[t]he harm suffered by [the debtor], namely, the mere prospect of a slightly less convenient discovery process . . . [was] not a concrete harm." *Id.* at 861. In reaching its conclusion, however, the Sixth Circuit discussed its prior opinion in *Galaria*, including its prior holding that the *Galaria* plaintiffs "satisfied the injury-in-fact requirement by alleging that the theft of their personal information constitutes 'a substantial risk of harm, coupled with reasonably incurred mitigation costs.'" *Id.* at 859 (quoting *Galaria*, 663 F. App'x at 385, 388). Notably, the Sixth Circuit distinguish *Lyshe* from *Galara* stating that "[u]nlike Lyshe, the plaintiffs in *Galaria* alleged a concrete harm arising from the violation of the statute—a risk that their data would be used for fraudulent purposes—rather than just a violation of the statute." *Lyshe*, 854 F.3d at 859 (citation omitted). Here, unlike *Lyshe*—and consistent with *Galaria*—Plaintiffs allege a concrete harm resulting from the Data Breach, i.e., a risk that their data would be used for fraudulent purposes.

This pronouncement was further echoed in *Saleh v. Barr*, 801 F. App'x 384, 386 (6th Cir. 2020), where children sought a declaration that agents of the FBI and USCIS conspired to prevent their father from obtaining citizenship, thereby exposing him to the threat of removal and exposing Plaintiffs to the risk of separation from their father. *Id.* at 390. The children argued that "the *exposure* to the risk of their father's removal [wa]s itself injury in fact, rather than his actual removal," but the Sixth Circuit rejected that argument, concluding that the children failed to satisfy the injury in fact requirement of Article III standing. *Id.* at 390-93 (emphasis in original). *See id.* at 392 (finding that the plaintiffs "do not allege any injury from reasonable efforts to mitigate a substantial likelihood of future harm," that "they do not allege any intended conduct in which they are prevented from engaging for fear of prosecution," and that instead, they "allege the purely psychic harm of worry about the possibility of their father's removal, which [they] have not shown

is likely to occur"). In reaching its decision, the Sixth Circuit discussed the "types of cases in which courts have held that a substantial risk of future harm alone constitutes a concrete injury in fact." *See id.* at 391. The Sixth Circuit highlighted how (1) "the Supreme Court has found that standing is satisfied when 'a reasonable probability of *future* injury comes accompanied with *present* injury that takes the form of reasonable efforts to mitigate the threatened effects of the future injury or to prevent it from occurring,'" *see id.* at 391-92 (emphasis preserved) (quoting Clapper, 568 U.S. at 437); and (2) "in the data-breach context, this Court has suggested that a '[p]laintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation.'" *Id.* at 392 (quoting *Galaria*, 663 F. App'x at 388).

District courts within the Sixth Circuit have also found *Galaria* to be consistent with current standing standards in the data breach context. For example, in *Allen v. Wenco Mgmt., LLC*, No. 1:23 CV 103, 2023 WL 6456571 (N.D. Ohio Sept. 29, 2023), a Wendy's employee brought a class action lawsuit against his employer as the result of a data breach. The defendant argued in part that dismissal was proper because Plaintiff failed to plead legally cognizable damages. *See id.* at *2. The defendant relied on *Jones v. Ohio Bureau of Workers' Comp.*, 2011-Ohio-1855 (Ct. Cl.), which held that an increased risk of identity theft was too hypothetical to confer standing. *See Allen*, 2023 WL 6456571, at *4. The court, however, stated that "the doctrine of Article III standing has come a long way since *Jones*—especially in the data-breach context," and, "for the reasons outlined at length in . . . *Galaria*, the court is confident that [the plaintiff]'s alleged increased risk of identity theft gives him standing to sue" the defendant. *Id.*; *see also Newman v. Total Quality Logistics, LLC*, 2021 WL 1192669, at *4 (S.D. Ohio Mar. 30, 2021) (applying *Galaria* and concluding that the plaintiffs' complaint "contains sufficient allegations to demonstrate that

Plaintiffs have suffered an injury in fact").

Furthermore, despite Defendant's argument that *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021) "casts some doubt on the continued viability of *Galaria*," (Def.'s Br., ECF No. 20, PageID.313-316), the Sixth Circuit has yet to reconsider *Galaria* in light of *TransUnion*, and recent case law from district courts within the Sixth Circuit suggest that *TransUnion* is distinguishable from *Galaria* because *TransUnion* involved a legitimate credit reporting company whereas *Galaria* involved a data breach by cybercriminals. *See Lochridge v. Quality Temp. Servs., Inc.*, No. 22-cv-12086, 2023 WL 4303577, at *4 (E.D. Mich. June 30, 2023) (finding that the Sixth Circuit has yet to officially reconsider *Galaria* in light of *TransUnion*, that *Galaria* more readily considered the unique threats present when information is obtained during a targeted cyberattack," and that, "applying the Sixth Circuit's rationale from *Galaria*, [the p]laintiff has alleged a sufficient injury in fact to support Article III standing"); *Brickman v. Maximus, Inc.*, No. 2:21-CV-3822, 2022 WL 16836186, at *4 (S.D. Ohio May 2, 2022) (finding that "the Sixth Circuit has not yet reconsidered *Galaria* in light of *TransUnion*," that *TransUnion* is distinguishable because it deals "with a legitimate credit reporting company while . . . *Galaria* . . . address[es] data breaches by cybercriminals, and that "*Galaria* controls"). Additional case law even suggests that *Galaria* is consistent with *TransUnion*. *See Bowen v. Paxton Media Grp., LLC*, No. 5:21-CV-00143, 2022 WL 4110319, at *5 (W.D. Ky. Sept. 8, 2022) (discussing how "*Galaria* is consistent with *TransUnion*").

Lastly, while it is true this Court in *Kingen v. Warner Norcross + Judd LLP*, No. 1:22-cv-01126-PLM-RSK (W.D. Mich.) recognized the split among circuits with respect to what constitutes a sufficient Article III injury in data breach cases, that *TransUnion LLC* casts some doubt on the continued viability of *Galaria*, and that the *Galaria* framework is at least persuasive

precedent, *see* Def.'s Mot., ECF No. 20, PageID.312, this Court also recognized that the continued viability of *Galaria* "is a question for the Sixth Circuit, not this Court." *See Kingen*, 1:22-cv-01126 PageID.109-110.

2. Plaintiffs Satisfy the Standing Requirements Set Forth by *TransUnion*

LCC incorrectly contends that Plaintiffs' alleged injuries "do not rise to the level of an injury in fact and the Complaint should be dismissed" under *TransUnion*. Def.'s Br., ECF No. 20, PageID.316. In *TransUnion*, a car dealer refused to sell the plaintiff a vehicle because a TransUnion-prepared credit report erroneously identified the plaintiff as being on a terrorist watchlist. *TransUnion*, 141 S. Ct. at 2201. The plaintiff sought to represent a class of *all* individuals who had been misidentified on such a credit report, regardless of actual dissemination to a third party. *Id.* at 2202.

While the Court found that individuals whose reports were never disseminated were not injured, the Court had "no trouble concluding" that *all* of those "class members whose credit reports were provided to third-party businesses suffered a concrete harm and thus have standing." *Id.* at 2209, 2214. The Court did not require a showing of additional harm resulting from TransUnion's sharing of inaccurate information with potential creditors to satisfy standing. It was sufficient for Article III standing purposes that the incorrect information was shared with a third party at all. *See id.*

Here, as in *TransUnion*, Plaintiffs' and Class Members' information PII was actually accessed. Here, by unauthorized individuals. *See, e.g.*, CAC ¶ 42. Upon information and belief, that PII was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type. *Id.*, ¶ 43. Any arguments to the contrary are subject to discovery and not suitable for a determination on a motion to dismiss.

Indeed, courts applying *TransUnion* in the data breach context – particularly in cases where, like here, an intentional breach followed by identity theft and fraud is alleged – have found such allegations to be sufficient for Article III standing. *See Kostka v. Dickey's Barbecue Rests., Inc.*, No. 3:20-CV-03424-K, 2022 WL 16821685, at *5 (N.D. Tex. Oct. 14, 2022), *report and recommendation adopted*, 2022 WL 16821665 (N.D. Tex. Nov. 8, 2022); *In re USAA Data Sec. Litig.*, 621 F. Supp. 3d 454, 464 (S.D.N.Y. 2022); *Salas v. Acuity-CHS, LLC*, No. CV 22-317-RGA, 2023 WL 2710180, at *6 (D. Del. Mar. 30, 2023) (citing *Clemens*, 48 F.4th at 155-56).

Accordingly, Plaintiffs' compromised information is more akin to the inaccurate credit reports shared with third parties in *TransUnion*—for which the Supreme Court had "no trouble concluding" that Article III was satisfied—than to the reports never shared. Plaintiffs' allegations here even surpass those found to be actionable in *TransUnion*, as Plaintiffs allege that malicious third parties intentionally targeted their PII in a deliberate hack (*see* CAC ¶ 10), and that this information ended up for sale on the dark web. *Id.* ¶¶ 43, 94. *See McMorris*, 995 F.3d at 302 ("allegations that the plaintiffs' PII was available for sale on the Dark Web following a data breach—and could therefore be purchased by cybercriminals at any moment to commit identity theft or fraud—provided strong support for the conclusion that those plaintiffs had established an Article III injury in fact"); *see also Dennis v. MyLife.Com, Inc.*, No. 20-cv-954, 2021 WL 6049830, at *4 (D. N.J. Dec. 20, 2021) (finding, under *TransUnion*, a plaintiff establishes standing by alleging that the defendant "disseminated private and/or inaccurate information about them to third parties through their website").

The focus on the inquiry at this stage in the proceedings is on the sufficiency of Plaintiffs' allegations in the CAC, not on LCC's self-serving statements that the PII "was not exfiltrated by the TA" and "has not been offered for sale nor distributed on the 'dark web.'" Def.'s Br., ECF No.

20, PageID.323. As discussed above, Plaintiffs have sufficiently pleaded actual data exfiltration, misuse, and tangible harm suffered as a result of the Data Breach. LCC's arguments to the contrary are based on factual disputes that cannot be resolved at the pleading stage. Plaintiffs sufficiently plead Article III standing.

C. Plaintiffs' Claims Survive Dismissal

1. Standard of Review Under Rule 12(b)(6)

When analyzing a motion to dismiss under Rule 12(b)(6), the court must "construe the complaint in the light most favorable to the plaintiff, accept its allegations as true, and draw all reasonable inferences in favor of the plaintiff." *Directv, Inc. v. Treesh*, 487 F.3d 471, 476 (6th Cir. 2007). To survive a motion to dismiss, a plaintiff must allege facts sufficient to state a claim for relief that is "plausible on its face" and, when accepted as true, are sufficient to "raise a right to relief above the speculative level." *Mills v. Barnard*, 869 F.3d 473, 479 (6th Cir. 2017) (citation omitted). "The complaint must 'contain either direct or inferential allegations respecting all material elements necessary for recovery under a viable legal theory.'" *Kreipke v. Wayne State Univ.*, 807 F.3d 768, 774 (6th Cir. 2015) (citation omitted).

2. Plaintiffs' Breach of Express Contract and Implied Contract Claims Survive Dismissal

Defendant's argument in favor of dismissing Plaintiffs' Breach of Express Contract (Count I) and Breach of Implied Contract (Count II) claims fails because Plaintiffs pleaded sufficient facts to adequately establish: (1) damages; (2) the inference of mutual assent between the parties for the purposes of the implied contract claim; and (3) that Defendant promised to honor its duties and obligations to protect Plaintiffs' and Class Members' PII. Accordingly, Defendant's request that the Court dismiss these claims must be denied.

First, contrary to Defendant's unsupported allegations, Plaintiffs' CAC is laden with

damages allegations, including loss of the benefit of Plaintiffs' and Class Members' bargain by overpaying for services that should have included a component of data security protection. CAC ¶¶ 12, 93, 121. Moreover, Michigan law expressly permits nominal damages for breach of contract claims:

> [N]ominal damages are generally sufficient to sustain a cause of action. "Nominal damages are those damages recoverable where plaintiff's rights have been violated by breach of contract or tortious injury, but no actual damages have been sustained or none can be proved."

4041-49 W. Maple Condo. Ass'n v. Countrywide Home Loans, Inc., 768 N.W.2d 88, 92 (Mich. App. 2009) (citing *Health Call of Detroit v. Atrium Home & Health Care Servs., Inc.*, 706 N.W.2d 843 (Mich. App. 2005) & 7 Mich. Civ. Jur. Damages § 9, at 313). Nominal damages alone defeats Defendant's argument that Plaintiffs have no legally cognizable damages to support their breach of contract claims.

Second, Defendant's attempt to attack Plaintiffs' breach of implied contract claim on the basis that Plaintiffs fail to allege sufficient facts to demonstrate mutual assent that LCC would take security measures protect Plaintiffs' and Class members PII is unpersuasive, primarily in light of LCC's own policy which promises exactly that.[5] Specifically, in the CAC, Plaintiffs quoted LCC's posted privacy policy which explicitly states: "LCC uses appropriate technical and organizational security measures to protect your information when you transmit it to the College and when the College stores it on its information technology systems." CAC ¶ 29. Plaintiffs further allege that "[t]his document was provided to Plaintiffs and Class Members in a manner in which it became

[5] Notably, Defendant excluded Plaintiffs' breach of express contract from its argument in favor of dismissal on this basis. *see* Def.'s Br., ECF No. 20, PageID.308 ("Moreover, even if Plaintiffs could meet the damages requirement, they have still failed to plead facts sufficient to support a breach of implied contract claim.").

part of the agreement for services and/or employment at LCC." CAC ¶ 189. In Michigan, pleading a breach of an express or implied contract claim does not require reference to any writing at all. *See Cascade Elec. Co. v. Rice*, 245 N.W.2d 774, 777 (Mich. App. 1976) (plaintiff "could seek recovery on the basis either of an express verbal contract, or an implied contract if the jury found that the express verbal contract did not exist" (citing *Fraser v. Collier Const. Co.*, 8 N.W.2d 889 (Mich. 1943) & *In re Moon's Est.*, 188 N.W. 457 (Mich. 1922)).[6]

Thus, the fact that Plaintiffs here plead the existence of a written document makes their contract claims more than sufficiently plead at this stage. *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 535 (M.D. Pa. 2021) ("Plaintiffs have referenced company-specific documents and policies to support a promise implied by the parties' conduct") (comparing to *Longenecker-Wells v. Benecard Servs. Inc*, 658 F. App'x 659, 663 (3d Cir. 2016) ("Plaintiffs here do not plead any company-specific documents or policies from which one could infer an implied contractual duty to protect Plaintiffs' information"); *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015) (same). Other data breach cases are in accord. *See In re Marriott*, 440 F. Supp. 3d at 484 (finding an implied contract on the basis of the defendant's privacy policy which promised the company would employ "reasonable organizational, technical and administrative measures to protect [its customers'] Personal Data.")*: Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 750 (S.D.N.Y. 2017) (the defendant's "privacy policies and security practices manual—which states that the company 'maintains robust procedures designed to carefully protect the PII with which it [is] entrusted'—further supports a finding of an implicit promise"); *Mackey*

[6] Defendant's reliance on *Kingen*, is misguided because, there, the plaintiff had alleged only the existence of a contract but none of its terms. That is not the case here and Plaintiffs' allegations are precisely those upon which courts sustain breach of contract claims at the pleading stage.

v. Belden, Inc., No. 4:21-cv-00149, 2021 WL 3363174, at *9 (E.D. Mo. Aug. 3, 2021) (upholding breach of implied contract to secure PII).

Lastly, Defendant's claim that Plaintiffs did not sufficiently plead consideration similarly fails. Plaintiffs plainly allege that they "paid money and/or provided their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security" and that they suffered "price premium damages." CAC ¶ 12, 93, 121, 202. Moreover, in addition to agreeing to work for Defendant, or enroll in classes, Plaintiffs and Class Members provided their PII to Defendant, which other courts recognize as sufficient consideration to form a contract. *Envolve Pharmacy Sols., Inc. v. Rite Aid Headquarters Corp.*, No. N19C-12-214 PRW CCLD, 2023 WL 2547994, at *14 (Del. Super. Ct. Mar. 17, 2023) ("No doubt there is a growing trend among courts to recognize the value of personally identifiable information. With regard to the Program, the Court views this personally identifiable information as sufficient consideration to create a valid contract."). Defendant, for its part, agreed to protect PII through its privacy policy. *See e.g.*, *Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561, 590 (N.D. Ill. 2020), *aff'd as modified*, 73 F.4th 502 (7th Cir. 2023). Accordingly, as each element of the contract claims is properly pleaded, Defendant's motion must be denied.

3. Plaintiffs Adequately Plead Unjust Enrichment in the Alternative

For the reasons set forth below, Plaintiffs sufficiently plead that they conferred benefits upon Defendant and that Plaintiffs and Class Members suffered Damages. Therefore, Plaintiffs' claim for unjust enrichment should not be dismissed at this stage.

Courts in the Sixth Circuit have recently denied motions to dismiss claims for unjust enrichment where plaintiffs allege a conferral of a monetary benefit upon defendants in exchange for products and/or services that did not match the defendants' representations of such products

and/or services. *See, e.g.*, *Tucker v. Marietta Area Health Care, Inc.*, No. 2:22-cv-184, 2023 WL 423504, at *7 (S.D. Ohio Jan. 26, 2023) (denying the defendant's motion to dismiss the plaintiffs' unjust enrichment claims where the plaintiffs allege to have paid beyond what was owed for medical treatment to ensure the security of their private information); *Bowen*, 2022 WL 4110319, at *8 (denying the defendant's motion to dismiss the plaintiffs' unjust enrichment claim where the plaintiffs alleged that the defendant knowingly enriched itself by the savings in costs that should have been reasonably expended to protect their PII).

Within the employment context, courts have also ruled that a benefit is conferred on an employer when an employee entrusts their personal information with the employer, and it is unjust for the employer to receive that benefit without taking adequate precautions to protect that information. *See, e.g.*, *Sackin*, 278 F. Supp. 3d at 751-52 (upholding a claim of unjust enrichment where an employer was enriched at employee's expense by not implementing security measures to protect employee's PII—which the defendant required or obtained in the course of employment.)

Here, Plaintiffs specifically allege a direct conferral of multiple benefits upon Defendant when Plaintiffs and Class Members (a) "provided their PII" to Defendant, and (b) "paid money" to Defendant "in connection with their admission applications." CAC ¶ 214. Plaintiffs further allege that employee Class Members provided their PII and labor to Defendant. *Id*. Plaintiffs allege that Plaintiffs and Class Members provided Defendant with these benefits based on the understanding that Defendant would use these benefits, in part, to fund adequate data security measures which, as alleged, are funded from the "payments made by or on behalf of [Plaintiffs and Class Members]" and/or "as a direct result of employment." CAC ¶¶ 213, 214. Thus, Plaintiffs allege Defendant "profited from these transactions and used the PII of Plaintiffs and Class

Members for business purposes[,]" enriching itself by "saving the costs it reasonably should have expended on data security measures . . . and instead direct[ing] those funds to its own profit. CAC ¶¶ 215, 216. These detailed allegations, at this stage, adequately demonstrate that it was unjust for Defendant to retain these benefits without taking proper precautions to invest in data security safeguards that would have protected Plaintiffs' and Class Members' PII from being compromised and its unauthorized disclosure as a direct and proximate result of Defendant's Data Breach. For these reasons, Plaintiffs adequately plead a claim for unjust enrichment.[7]

Defendant also wrongly contends that Plaintiffs rely on speculative future damages to support their unjust enrichment claim. Def.'s Br., ECF No. 20, PageID.310. As set forth *supra*, Plaintiffs' allegations of damages, including those suffered as a result of Defendant's unjust enrichment, go beyond "speculative" and are recognized by courts across the country as cognizable injuries-in-fact within the data breach context, thus rising above the speculative level. For these reasons, Defendant's motion to dismiss Plaintiffs' unjust enrichment claim should be denied.

[7] Defendant misinterprets the caselaw it cites at PageID.309-310, stating that such rulings stand for the proposition that Plaintiffs must plausibly allege "what benefit LCC has retained by possessing Plaintiffs' PII *or through the data breach*" (emphasis added). Plaintiffs, however, need not allege what benefit LCC has retained through the Data Breach; such a requirement is unreasonable given that it is unlikely that a party would gain any benefit from a malicious breach of its network. Plaintiffs must only plausibly allege (and do allege) LCC's receipt of a benefit from Plaintiffs, and an inequity resulting from Defendant's unjust retention of said benefit. *Belle Isle Grill Corp. v. Detroit*, 666 N.W.2d 271, 280 (Mich. App. 2003). The cases cited by Defendant are also distinguishable in that the plaintiffs in those cases did not allege, beyond conclusory allegations, any direct payment made to the defending parties or how defendant was benefitted. *See, e.g.*, *Kingen* (granting motion to dismiss unjust enrichment claim, observing the conclusory nature of the plaintiffs' allegations regarding the benefits conferred upon the defendant). Here, however, Plaintiffs plead detailed allegations, exceeding those made in *Kingen*, regarding the direct monetary payments and transfer of highly valuable personal information and labor provided to Defendant and how Defendant was unjustly enriched by retaining such benefits. *See* CAC ¶¶ 212-216.

V. CONCLUSION

Plaintiffs, individually and on behalf of the Class, adequately plead their claims and the Court should deny Defendant's motion to dismiss in its entirety. To the extent that the Court deems it necessary, Plaintiffs pray for leave to amend their Complaint.[8]

November 10, 2023

Respectfully Submitted,

/s/ Benjamin F. Johns
Jonathan Shub
Benjamin F. Johns
Samantha E. Holbrook
SHUB & JOHNS LLC
Four Tower Bridge,
200 Barr Harbor Drive, Ste
400 Conshohocken, PA 19428
T: (610) 477-8380
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Nick Suciu
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301
Tel: (313) 303-3472
Email: nsuciu@milberg.com

E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300

[8] Plaintiffs acknowledge that if the Court deems such an amendment necessary, procedurally, Plaintiffs will be required to file a formal motion for leave with an attached proposed amended complaint.

Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

**pro hac vice to be filed*

Attorneys for Plaintiffs and the Putative Class

CERTIFICATE REGARDING WORD COUNT

Plaintiffs, in compliance with W.D. Mich. LCivR 7.2(b)(i)-(ii), used 9,321 words in Plaintiff's foregoing brief. Microsoft Word for Office 365 Business version 1910 is the word processing software used to generate the word count in the attached brief.

November 10, 2023

Respectfully Submitted,

/s/ Benjamin F. Johns
Benjamin F. Johns
SHUB & JOHNS LLC
Four Tower Bridge,
200 Barr Harbor Drive, Ste
400 Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com

CERTIFICATE OF SERVICE

I hereby certify that on November 10, 2023, I electronically filed the foregoing document(s) using the Court's electronic filing system, which will notify all counsel of record authorized to receive such filings.

/s/ Benjamin F. Johns
Benjamin F. Johns
SHUB & JOHNS LLC
Four Tower Bridge,
200 Barr Harbor Drive, Ste
400 Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com